

IN THE SPECIFICATION

Amend the paragraph extending between pages 1 and 2 as follows.

Q1 Although information is mostly managed by a computer nowadays, spilling and leakage of information are often conducted using paper. While paperless work is advocated lately, consumption of paper in offices is recently rather increasing in the form of printout from computers. Furthermore, diffusion of the office appliances ~~OA devices~~ such as copiers and faxes brought about a situation in which spilling of information can easily occur. Under such circumstances, a technical means to prevent paper-based spilling and leakage of information and to trace any spilled and leaked document is required.

Amend the three paragraphs extending from page 2, line 17, to page 3, line 20, as follows.

Q2 For instance, Japanese Unexamined Patent Publication No. Hei7-84485, abandoned without request for examination, discloses a technique for embedding a watermark to identify an output device of a copier, and this technique implements embedding by changing brightness of the yellow toner in two or more areas placed on the entire page. As a matter of course, scanning of a colored and multivalued image is required to detect it, but documents are generally not multivalued but black and white binary, and it is not practical cost-wise to go to the extent of adding a function for capturing a color image to a black and white copier or a fax in order to detect a watermark.

Japanese Unexamined Patent Publication No. Hei6-324625, abandoned without request for examination, discloses a technique for embedding a watermark by means of subtle differences in shape such as a touch of a character. However, an image scanned after printing on paper has changed from the original image at a pixel level since it is influenced by the type of a

02 printer's printing mechanism and the difference in resolution between a printer and a scanner. In addition, there are also changes due to establishment of density and how the document is written such as misregistration or skew (slant of paper) on copying, printing and scanning, and an effect of noise such as stains and blurs. It is difficult to stably detect, among these changes, a local change in shape due to embedding.

Japanese Unexamined Patent Publication No. Hei7-222000, now Japanese Patent 3,136,061, discloses a technique for embedding a watermark by increasing and decreasing vertical intervals of a center line in text lines. This technique can endure the scan after printing, but it cannot be applied to the above-mentioned scenario for preventing spilling and leakage since it requires the information extracted from the original document on detection.

~~Amend~~ the paragraph extending between pages 9 and 10 and the first full paragraph on page 10 as follows.

03 As for the detected set of rectangles circumscribed around the lines, each rectangle is split into subblocks, and the subblocks are divided into two groups. Splitting and grouping can be randomly determined, as far as the same ones are used in embedding and detecting a watermark. However, the following are desirable to enhance likelihood of detecting watermarks, namely to stably detect a watermark.

1) There is no significant difference in the total sums of the area of the blocks belonging to each group.

2) If a line rectangle is split into upper and lower portions, the upper and lower subblocks belong to separate groups respectively.

23) This has an effect of setting off an element that changes the features used in embedding, such as influence in a case where the Gothic type is partially used in text of the Mincho typeface.

Fig. 3 shows an example of splitting and grouping of a line rectangle. In this example, a rectangle circumscribed around the text line of "Globalization of business activities and consumers' rights" is horizontally divided into six equal parts, and vertically divided into two equal parts so as to be totally divided into 12 subblocks. (1) and (2) of Fig. 3 (c) indicate the groups that the subblocks belong to, namely they are grouped into two kinds of (1) and (2).e

Amend the paragraph extending between pages 11 and 12 as follows.

It is also possible, by way of another example, to utilize average thickness of a line segment as a feature. Fig. 8 shows a flowchart of detecting an average thickness of a line segment. As shown in Fig. 9, thickness is detected by performing a raster operation at 81 on a subject rectangular area of which primary operational direction is vertical. A program for detecting thickness information observes each vertical scan line and detects a run of black pixels, and then converts it into run data (information of a viewpoint and length) at 81. Length of each run is compared with a threshold of which length is predetermined at 82, and the length and number of the shorter run is recorded at 83. When the raster operation is complete at 86, an average run length is calculated. In the flowchart of Fig. 8, a horizontal line segment or a line segment close to horizontal are the subjects for detection. Length is compared with a threshold at 82 in order to consider as subjects for counting only the runs crossing from above a horizontal line segment or a line segment close to horizontal. Figure 8 is a flowchart for detecting features such as the thickness of a line segment. The operation starts at 80 with total len (length) <-0, and run num (number) <-0. A first vertical line is then converted into scan run data at 81, and at 82

a4
the length of the run is checked to determine if it is shorter than a threshold. If Yes, at 83
increment total len <- total len and run length, and run num <- run num +1. If No, bypass 83,
and at 84 determine if the length of all of the runs on the scan line have been checked. If No,
return to 82 to check the length of the next run. If Yes, proceed to 85 to determine if all of the
vertical lines have been scanned. If No, return to 81 to convert the next vertical line to scan run
data. If Yes, determine at 86 the result <- total len/run num.

Amend the paragraph extending between pages 16 and 17 as follows.

a6
Fig. 6 shows, as an example of application of contents identification, a frame for managing confidentiality of document 60 (stored in files 61) information by using the present invention. A function of embedding a watermark is incorporated into the printer 62 in the diagram, and a function of detecting a watermark is incorporated into the fax 63 and copier 64. When printed by a printer, an authorization bit of faxing or a copying is embedded into a document as a watermark. When this document is about to be copied or faxed, watermarking information is checked in scanning, and the process is continued if the authorization bit is on as at 65, whereas the process is terminated at 66 or a record (the user, object, etc.) is kept if the authorization bit is off as at 67. Thus, the present invention can prevent a paper document from being wrongfully duplicated or spilled by a copier or a fax. In general, an original paper document is managed relatively in a strict manner so that there is a high possibility, if the original is taken out, of discovering the fact of being wrongfully taken out when using (reading) the document next time, whereas tracing and managing a duplicated document is difficult. For the party taking it out, the psychological barrier is low in the sense that "the document was not stolen." In fact, a copier or a fax is used in many cases of wrongful information spilling. The

95
frame provided by the present invention can check validity of the action when a duplicate is made so that it is highly effective in prevention of wrongful spilling of paper documents.

Amend the paragraph extending between pages 17 and 18 as follows.

AM
Fig. 7 shows a frame for preventing forgery of a document by using the present invention. An issuer 70 of an authentic document 71 uses a printer 72 with a watermark embedding function to print and circulate a document. Subject documents for a watermark embedding can be economic information that may influence action of others, certificates, tickets and so on. Contents of a watermark, how to split into and group subblocks on embedding and setting of the features are to be kept only by the issuer. If it becomes necessary to verify authenticity of a document, a document image can be sent to the issuer via fax 73 or the Internet 74, requesting determination as to whether or not a watermark can be properly detected. Even if a forger 75 knows the algorithm of a watermark embedding or has a printer 76 with a watermark embedding function, a forger cannot embed into a document 77 or detect the same watermark as far as how to split into and group subblocks and setting of the features are kept secret only to the issuer.

Amend the Abstract on page 24 as follows.

ME
As a document image on paper is usually black and white binary data, an embedding method for colored and multivalued data using a variation of light and dark could not be applied. When a document printed on paper was captured by a scanner or the like, it was difficult, since it had changed at a pixel level, to stably detect embedded additional watermarking information. A text area is detected from a document image, and the features of the detected text area are increased or decreased, or the detected text area is split into two or more subblocks, and the said subblocks are divided into two or more groups, of which features are increased or

decreased respectively so as to embed additional watermarking information. ~~so that, w~~ When detecting a watermark, additional watermarking information is detected by comparing the integrated values of the features acquired from the respective groups.